

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-162601
(43)Date of publication of application : 06.06.2003

(51)Int.Cl. G06F 17/60
G06F 12/14
G06F 15/00

(21)Application number : 2002-237927 (71)Applicant : HEWLETT PACKARD CO
<HP>
(22)Date of filing : 19.08.2002 (72)Inventor : ERICKSON JOHN S
SCHLAGETER MARK

(30)Priority
Priority number : 2001 941615 Priority date : 30.08.2001 Priority country : US

(54) PROXY SERVICE PROVIDING APPARATUS

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an apparatus providing proxy service between a client platform and a remote contents provider providing electronic contents.

SOLUTION: The apparatus is provided with a means to receive and interpret requests for electronic contents of the contents provider from the client platform a means to transmit the requests to the contents provider and receive data including at least one marker indicating locations of information operating/policy performing remote servers suitable for the requested contents and a means to interpret the one or more markers and transmit instead of the client platform requests for transmitting a clear contents version of the contents to the client platform when requirements of information operating/policy performing service are satisfied.

CLAIMS

[Claim(s)]

[Claim 1] It is a device which provides proxy service between one or more client plat forms and one or more remote plat forms(a) Receive and interpret a demand

of a client platform to electronic contents or information on a remote platform. A function to transmit said demand to said remote platform and to receive data or (b) -- a means to perform both both [either or] which receive data which is typical information or contents with which said remote platform is provided from a client platform [have and] Said data includes at least one marker showing a location of manipulation of information / policy operation remote service suitable for information or contents required or provided.

When said one or more markers are interpreted and requirements for manipulation of information / policy operation service are satisfied, said device (a) A function which transmits demand of providing said client platform with said information or a clearance contents version of contents instead of said client platform or (b) -- a proxy service provision system constituted so that it might have a means to perform both both [either or] which transmit demand of providing said remote location with said information or a clearance contents version of contents to suitable manipulation-of-information policy operation service.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] Especially this invention relates to the flexible platform which supports the right management method and other manipulation-of-information policies only for an information technology network environment concerning electronic right management generally.

[0002]

[Description of the Prior Art] Copyright is intellectual property rights granted to the original author of a specific kind of work and the original author can manage various directions of the work according to copyright. Copyright is for protecting literature, a drama, music, the work of fine arts, a publication, sound recording, a movie (video is included) and the original of broadcast (cable broadcasting and satellite broadcasting are included).

The right provided by copyright reaches various fields such as a duplicate of the work which is the target of protection, adaptations, distribution of a duplicate, a public performance and broadcast.

In many cases, an author has the right to have it specified that it is its own work and the right to make an opposition to defamation and modification of its own work. Since the right of loan is given to sound recording, a movie and the copyright person of a computer program, the license delivered by the copyright person for carrying out by lending out such a work publicly is needed.

[0003] In recent years, electronic preservation of contents such as sound recording, a literary work and a movie is becoming increasingly general and commercial distribution of such electronic content is performed from the former at retail

stores such as a record shop and a bookstore. Although there are many advantages in the commercial distribution of the electronic content through an information technology network it is not necessarily widely adopted as the author or the distributor of such contents. The main Reason is concern of a third party reproducing and selling and becoming easy to distribute such contents unlawfully as a result. For this reason great efforts have been paid towards development of the technical protection measure of preventing the unjust duplicate of electronic content.

[0004] An illegal duplicate is comparatively easy and for a content provider this [digital contents'] is also convenient and is also inconvenient. That is although it is desirable that contents can be distributed by one side as widely as possible (value increases and it counts also upon acquisition of big profits) payment is wanted to still be made certainly for every sale. i.e. do not infringe on copyright. In order to prevent the above copyright infringement a content provider tends to adopt a digital protection method (usually based on encoding technology). This method is b with difficult restriction of distribution that it is hard to use for a consumer. There is a possibility that it may be cancelled by the free illegal method with which a user tends to operate the contents of c EQC which requires expense for management.

[0005] One of the known protection methods is provided from Microsoft Digital Media System and electronic content is provided with a key. The user cannot reproduce contents unless it acquires a key corresponding from a regular key server. The main faults of this method are that the connection with a user's playback equipment is strong. That is when reproducing the contents protected by this method a device for exclusive use is needed.

[0006] Generally substantial encryption of the work is included in known digital rights management and protection method.

Reproduction of the contents reproduced and reproduced is difficult.

The digital-rights-management (DRM: Digital rights management) art used now is known by the user also as a secure container. That is by this art an original file format is defined and arbitrary media files are encapsulated to secure one in it.

[0007] For example the art for defining using and operating a right management data structure to US6138119B is shown. In this Description safe and secure preservation and transmission of digital contents are realized using the concept of a secure digital container. Since an alteration is difficult for such a container the digital information of arbitrary form such as a text graphics software that can be performed an audio and video can be used for package-izing for example. However the situation where secure contents can be used is limited by this method.

[0008] In another system plug-in security function is provided to specific media formats (Adobe (trademark) PDF etc.). A software plug-in business model Video an audio (connectable codec) multimedia (connectable execution program "extends" a program) Although the Creativity tool (filter which extends the Image Processing Division tool) a web browser etc. have been used for extension of application over many years in other specific commercial scenes only Adobe Acrobat (trademark)

provides the security function now.

A third party's developer can develop uniformly DRM which functions in a specific format using Acrobat TM.

However the method of using it by this system is restricted by the function of a target format (PDF). That is by this method the format which can guarantee security is limited to one kind and the kind of media is limited.

[0009] The provider of digital information products a broker and consumers An information producer presents intellectual property rights (IPR) and it is afflicted by "fragmentation of policy operation" without the consistent platform which asserts an IPR policy (policy showing the rule to which brokers such as a wholesaler a retailer and a library operate information especially). Displaying such information for users the platform where it was [for interpreting and carrying out a policy] consistent does not exist. The consumer in connection with transmission of private data and reuse releasable in the middle of a network transaction is not necessarily carrying out the policy which prepares the too consistent platform and operates individual information under the control either.

[0010] Generally the user in connection with an information value chain wishes to receive information after presenting the policy about handling or processing of information thought to be a policy demanded about the handling of the information to operate. In known art this problem is unsolvable by the consistent systematic method.

[0011] The concept of using proxy service for filtering of contents and adaptation is known (a "proxy" only means "the authority which the substitute was given" in a broad sense). For example filtering based on the rule for removing the advertisement etc. of contents which are not desirable is the newly generated work. By removing specific data from the data which a computer receives especially via a network at US5996011B with a filter has described the system and method of restricting access to the received data. The method of the computer base which filters the text data or the target text data which is not preferred from the World Wide Web page which the computer connected to the Internet receives is shown by one embodiment. In the Internet or Internet environment in US6119165BA function is added to the proxy server which supports many clients and there is description about the system which enables it to provide a specific client with a software module based on the characteristic of a client. In this way the downloaded module is performed by the client which set up the two-way communication link of a proxy server and a client. With a bidirectional link the status display in the client side which uses the window of a client platform for example becomes possible and a virus scan filtering of contents bandwidth use etc. can display the present status of a proxy server. In other applications the offer origin of the bulletin board of an organization a news channel and a common software patch can be built with the downloaded module.

[0012] It is acquired from the Internet computer network with the server of a remote Internet Service Provider by US5987606B The system which filters the Internet contents transmitted to a local client computer is shown. At least one

filtering methodssuch as a filter implicative in this systemand an exclusive filterAt least one filtering elementssuch as a list of the site permitted or sites which are exceptedare compared with the specific Internet requests generated with the local client computer. In this casealthough the filtering method is mounted in the ISP servergenerally this kind of filtering service and adaptation service may be applied to any of the halfway point of a client sidea serverand both. It is not necessary to limit filtering and adaptation to downstream contents (contents which a client plat form receives from a server). That isin order to guarantee privacy and anonymitythe proxy service which is adapted for a user input exists.

[0013]

[Problem(s) to be Solved by the Invention]Howeverno known proxy services provide the practical intervention point of application (they are management of copyrightand service of use especially) of a manipulation-of-information policy. By the known mechanism which generally carries out a copyright policyas above-mentioned. Usually, [whether a result which uses special "read-out" software by the client sideand spoils pleasure of the end user about contents is broughtand] The policy operation function for which it depends on very restrictive contents by the server side will be usedand the contents which can appreciate an end user will be restricted. Client application for exclusive use has many faults from restriction by plat-form compatibility or application compatibility to a user's inconvenience. There are many weak points also in the system of a known server base from the problem of the granulation on management to the problem of the pliability of contents.

[0014]

[Means for Solving the Problem]Thenstructure for conquering the above problem was devised. In this wayaccording to the 1st side of this inventiona device which provides proxy service between one or more remote content providers who provide one or more client plat formselectronic contentsor information is provided.

[0015]A means for this device to receive a demand of a client plat form to a content provider's electronic contentand to interpretA means to receive data including at least one marker showing a location of the manipulation of information / policy operation remote server which transmitted said demand to a content provider and was suitable for demanded contentsSaid one or more markers are interpretedWhen requirements for manipulation of information / policy operation service are satisfiedit has a means to transmit demand of transmitting a clearance contents version of said contents to said client plat forminstead of said client plat form.

[0016]According to the 1st side of this inventiona method of providing proxy service between one or more remote contents servers which provide one or more client plat forms and electronic content is also provided. A step which receives and interprets a demand of a client plat form to electronic content of a contents server in this methodA step which receives data including at least one marker showing a location of manipulation of information / policy operation remote server suitable for contents required as a step which transmits said demand to a

contents serverA step which interprets said one or more markersWhen requirements for manipulation of information / policy operation service are satisfied a step which transmits demand of transmitting a clearance contents version of said contents to said client plat form instead of said client plat form is contained.

[0017]According to the 2nd side of this inventionA device which provides proxy service between one or more remote plat forms adjusted so that electronic contents or information might be received from one or more client plat form and said one or more client plat forms is provided. This deviceAt least one marker showing a location of the manipulation of information / policy operation remote server to which data transmitted to a remote plat form fitted information which is typical information or contents with which said remote plat form is providedand is provided. A means to receive said data from a client plat form when containedA means to interpret said one or more markersWhen requirements for manipulation of information / policy operation service are satisfied it has a means to transmit demand of providing said remote location with a clearance contents version of said information to suitable manipulation-of-information policy operation service.

[0018]According to the 2nd side of this inventionA method of providing proxy service between one or more remote plat forms adjusted so that electronic contents or information might be received from one or more client plat form and said one or more client plat forms is also provided. In this method. When it includes at least one marker showing a location of the manipulation of information / policy operation remote server to which data transmitted to a remote plat form fitted information which is typical information or contents with which a remote plat form is providedand is providedA step which receives said data from a client plat formA step which interprets said one or more markersWhen requirements for manipulation of information / policy operation service are satisfied a step which transmits demand of providing said remote location with a clearance contents version of said information to suitable manipulation-of-information policy operation service is contained.

[0019]Thusthis invention provides proxy service which can be used as a relay point of a client plat form and various content providers accompanied by various right management policies or a manipulation-of-information policyThe content provider can carry out an original policy of his company certainly by it. Thereforethis invention provides proxy service which a client plat form and a client plat form can use as a relay point with various remote locations which transmit high information and individual information on confidentialityAn original policy about the confidentiality/anonymity of a client plat form is certainly maintainable by it. One proxy service according to this invention can be used for the two purpose. That issuch service can be adjusted so that both data received from a client plat form and data transmitted to a client plat form may be processed.

[0020]This proxy service may be locally arranged on a client plat form. Howeverwhen a "client" is provided with a systematic network including two or more plat formsthis proxy service may be arranged at the center in the network.

Or this proxy server may be arranged on a remote point of information technology networkssuch as the Internet.

[0021]A contents server returns a data stream which answers a contents request from this proxy serviceand includes one or more markers. Detailed information (URLDOIetc.) of a location of other services of one or more which needs to have a dialog before proxy service transmits a duplicate of contents to a client plat form is included in a marker. As for such a marker being embedded at a data streamthis being recognizedand it being able to interpretit is preferred to be limited to a means for exclusive use provided inside proxy service.

[0022]A client plat form in the case of a web browser etc.As for proxy servicewhen transmitting a contents request to manipulation of information / right management remote serverit is preferred to be adjusted so that data (session ID etc.) relevant to a client plat form may be included in a demand (directly or indirectly). Thereforemanipulation of information / right management remote server is provided with information about a client plat form. Detailed information peculiar to an end user can also be included in a demand (especially). When there are no special requirements relevant to manipulation of information / right management server for an end user and a client plat form to be another entitiesand for a client plat form converse with an end user.

[0023]If manipulation of information / right management server receives a contents request from proxy service and verifies the legitimacy of a demandManipulation of information / right management server creates a clearance contents version of contentssaves this for a local or a remote specific location (temporarily [if it can do])and returns detailed information of said location to proxy service further. As for proxy serviceit is preferred that it can adjust so that detailed information of a location of a client plat form which saves a clearance contents version of contents may be transmitted. When specific requirements about manipulation of information / right management server are satisfied by thisthe client plat form can acquire a duplicate of said clearance contents.

[0024]It cannot be overemphasized that a policy which manipulation of information / right management server adopts is dependent on character of contents required as a content provider (a natural thing *****). It is also clear that a client plat form or an end user can relate and do manipulation of information / right management service. After operating information transmitted to a remote location from a client plat form by a proxy server and processing via suitable manipulation-of-information service by thisit can transmit to said remote location.

[0025]

[Embodiment of the Invention]Hereone embodiment of this invention is explainedonly referring to attached Drawings as an example.

[0026]Reference of drawing 1 shows the typical connection (one example) between the web browser 10 (accessible from a client computer plat form (not shown))the proxy server 12 according to this inventionand digital-rights-management (DRM) Web Service 14. This connection is usually made via information technology networkssuch as the Internet. The arrows

122a33a44a4b4c4d56 and 7 show the direction of the demand and response which are exchanged in the typical process described below between the web browser 10, the proxy server 12, and DRM Web Service 14.

[0027] In the first instance when peculiar session ID is generated, the web browser 10 logs in to the proxy server 12. Session ID is not recognized by the end user but is used for verification of a session in a next process.

[0028] If the arrow 1 is referred to the display side client 10, i.e. a web browser, it will require a network resource by showing the proxy server 12 a network address (for example URL and DOI). It cannot be overemphasized that the proxy server 12 can be arranged [the network of a company or an organization] also on the remote point of information technology network, such as the Internet, also locally intensively to a user's workstation.

[0029] The proxy server 12 uses an HTTP protocol and usually transmits the suitable network request to a resource to the contents server 16 (arrow 2). The contents server 16 usually exists in location with the another proxy server 12 and returns resource, such as a Web page (arrow 2a). Generally a resource takes the form of an HTML file or a more general XML file. At the resource file, the thing similar to the markup tag which calls other resources is embedded and it can acquire only by processing for exclusive use in which the manipulation-of-information policy or digital rights management which the proxy server 12 provides was followed. This kind of markup tag is described as a <DRM> object by this embodiment of this invention. Such a <DRM> object instance in a data stream with "open" others transmitted to the proxy server 12. It has the attributes (URL, DOI, etc.) which refer to other Web resources which need to have a dialog in order for the proxy server 12 to embed and to check the location of the clearance (that is not enciphered) version of a contents object.

[0030] It cannot be overemphasized that the proxy server 12 is adapted for the markup tag embedded in the data stream received from the contents server 16. Even if the web browser 10 tends to acquire an immediate-data stream from the contents server 16 without passing the proxy server 12 first, only a portion with an "open" stream can recognize a browser. Therefore, neither recognition nor an interpretation can do a markup tag (that is, the web browser 10 disregards a tag).

[0031] If a resource-data stream is received from the contents server 16, the proxy server 12 will check the stream which received in accordance with a series of generated rules and will detect one or more markup tags embedded at the data stream. The proxy server 12 is adjusted so that the property which shows the location of the "drm file" arranged at the remote point on the Internet, for example, may be extracted from the tag text. Next, the proxy server 12 requires the specified <DRM> file (one or more) (arrow 3) and receives (arrow 3a). In the <DRM> file, XML syntax may be used, for example. The proxy server 12 extracts "content_type" and "content_location" (for example URL) of a actual contents object (usually package-ized by the secure container etc.) from this file.

[0032] This service interprets content_type which usually uses "MIME" encodings (image/jpeg etc.) and compares it with one or more content_type which registered

this content_type into proxy service. If content_type is one of the types registered into service a "clear" tag structure returned to an end user will be determined. For example when the package-ized contents are a MIME type image / jpeg the changed tag structure must be the format of "." That is when an end user enables it to use a resource (as a user to whom the registered user and the license were given) the proxy server 12 operates as follows.

[0033] Here it is required that the proxy server 12 should create a "clear contents" version peculiar to the session of the resource with which remote DRM Web Service 14 was specified and should return URL peculiar to a session (arrow 4). If it describes in detail drm service Interface Division 18 will arrange the encryption version of a <drm> file to the enciphered content archive 20 in drm Web Service 14 (arrow 4a). Next the contents archive 20 transmits the enciphered <drm> file to the decipherment component 22 which exists in drm Web Service 14 too. The decipherment component 22 decodes a file and creates a "clear contents" version. This clear contents version uses a peculiar file name peculiar (it is temporary) to a session and a cash advance is transmitted and (arrow 4c) carried out to the clear contents cash 24 which exists in drm Web Service 14 too. It is transmitted to drm service Interface Division 18 and a peculiar file name generates URL peculiar to the session of the resource which is not secure and transmits to the proxy server 12 (arrow 4d).

[0034] The proxy server 12 creates the contents stream (for example HTML page) changed using the format corresponding to MIME (in this case). A HTML page is reformatted so that URL of a meaning peculiar to a session which drm Web Service 14 provides may be specified. The reformatted HTML page is returned to the web browser 10 here (arrow 5).

[0035] Next the web browser 10 requires the contents which are saved via the redirector service interface 26 into the clear contents cash 24 in drm Web Service 14 and which are not secure (arrow 6). The demand of a browser comprises a query string who contains URL peculiar to an effective session only in the present browser session. Redirector service Interface Division 26 is compared with URL peculiar to a session described by the query string whom checks the present browser session and the browser 10 transmits. If a session is in agreement and the memory of clearance contents has a timeout rule when the term has not expired redirector service Interface Division 26 transmits clearance contents to the web browser 10 and the end user can use this.

[0036] This invention is based on the new concept of intervention of a proxy base and adaptation of contents and provides the platform which summarizes an interpretation and operation of a manipulation-of-information policy and a digital-rights-management policy. In the case of a portal etc. especially this is effective. In such a situation a user needs to apply a policy by the consistent flexible method to the large-scale base of the relation which uses various display ring boundaries. If it puts in another way and this invention will be used manipulation-of-information policies (policy of copyright use etc.) peculiar to a user can be consistently applied on the heterogeneous network of an organization.

[0037]In the technique adopted by this invention user authentication and the process of approval and actual mounting of policy operation of a mechanism are maintained independently intrinsically. By this an organization or the contents service can manage an information policy using the company database of central control (when various policies are applied to various rolls of especially an in-housesuch as a site licence of the organization about an electronic journal).

[0038]The above portion of a Description has described this invention in relation to the specific typical embodiment. However unless it deviates from the pneuma and the range of this invention which are shown in the above-mentioned claim it is clear to a person skilled in the art for the various modification and change to be possible. Therefore it is necessary to consider that does not mean restriction and this Description and Drawings mean illustration.

[0039]This invention contains the following embodiment as an example.

[0040](1) It is a device which provides the proxy service (12) between one or more client plat forms (10) and one or more remote plat forms (16)(a) Receive and interpret the demand of a client plat form (10) to the electronic contents or information on a remote plat form (16)The function to transmit said demand to said remote plat form (16)and to receive dataOr (b) It has a means to perform both both [either or] which receive the data which is the typical information or contents with which said remote plat form (16) is provided from a client plat form (10)Said data includes at least one marker showing the location of manipulation of information / policy operation remote service (14) suitable for the information or contents required or providedWhen said one or more markers are interpreted and the requirements for manipulation of information / policy operation service are satisfied said device(a) The function which transmits the demand of providing said client plat form with said information or the clearance contents version of contents instead of said client plat form(b) Said device provided with a means to perform both both [either or] which transmit the demand of providing said remote location with said information or the clearance contents version of contents to suitable manipulation-of-information policy operation service.

[0041](2) The data stream which answers the demand of the information by proxy service (14) or contents and includes one or more markers is returnedA device given in (1) in which the detailed information of the location of other services of one or more which needs to have a dialog before proxy service (12) transmits the duplicate of contents to a marker on a client plat form (10) is included.

[0042](3) A device given in (2) which the marker is embedded at the data stream can recognize a marker only by the means for exclusive use provided inside proxy service (12) and can be interpreted.

[0043]A client plat form (4) In the cases of a web browser (10) etc. When transmitting information or a contents request to manipulation of information / right management remote service (14)A device given in either of (1) to (4) adjusted so that proxy service (12) may contain the data relevant to client plat forms (10) such as session ID in a demand.

[0044](5) If manipulation of information / right management service (14) receives a

contents request from proxy service (12) and verifies the legitimacy of a demandA device given in either of (1) to (4) which creates the clearance contents version of contentssaves for a local or a remote specific location (24)and returns the detailed information of said location to proxy service (12) further.

[0045](6) A device given in (5) the clearance contents version of said contents is temporarily remembered to be.

[0046](7) It is adjusted so that proxy service (12) may transmit the detailed information of the location of a client plat form (10) which saves the clearance contents version of contentsAs a resulta device given in (5) from which a client plat form (10) can acquire the duplicate of said clearance contents when the specific requirements about manipulation of information / right management service (14) are satisfied.

[0047](8) It is the method of providing the proxy service (12) between one or more client plat forms (10) and one or more remote plat forms (16)(a) Receive and interpret the demand of a client plat form (10) to the electronic information or contents of a remote plat form (16)The step which transmits said demand to said remote plat form (16)and receives data(b) Both both [either or] which receive the data which is the typical information or contents with which said remote plat form (16) is provided from a client plat form (10) are includedAt least one marker showing the location of manipulation of information / policy operation remote service (14) suitable for the information or contents with which said data was required or provided is includedWhen the requirements for the step which furthermore interprets said one or more markersand service (12) of manipulation of information / policy implementation are satisfied(a) The step which transmits the demand of providing said client plat form (10) with said information or the clearance contents version of contentsinstead of said client plat form (10)(b) A method containing both both [either or] which transmit the demand of providing said remote plat form (16) with said information or the clearance contents version of contents to suitable manipulation-of-information policy operation service (12).

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a flow chart showing the outline of operation of the typical embodiment of this invention.

[Description of Notations]

10 Client plat form

12 Proxy service

14 Manipulation of information / right management remote service

16 Remote plat form

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2003-162601

(P2003-162601A)

(43)公開日 平成15年6月6日(2003.6.6)

(51)Int.Cl. ⁷	識別記号	F I	ターマコード [*] (参考)
G 0 6 F 17/60	1 4 2	G 0 6 F 17/60	1 4 2 5 B 0 1 7
	3 0 2		3 0 2 E 5 B 0 8 5
12/14	3 2 0	12/14	3 2 0 A
15/00	3 3 0	15/00	3 3 0 Z

審査請求 未請求 請求項の数1 O L (全 8 頁)

(21)出願番号 特願2002-237927(P2002-237927)

(22)出願日 平成14年8月19日(2002.8.19)

(31)優先権主張番号 09/941,615

(32)優先日 平成13年8月30日(2001.8.30)

(33)優先権主張国 米国 (U S)

(71)出願人 398038580

ヒューレット・パカード・カンパニー
HEWLETT-PACKARD COM
PANY
アメリカ合衆国カリフォルニア州パロアル
ト ハノーバー・ストリート 3000

(72)発明者 ジョン・エス・エリクソン

アメリカ合衆国05055バーモント州ノーウ
イッチ、132・ルード 707

(74)代理人 100081721

弁理士 岡田 次生 (外2名)

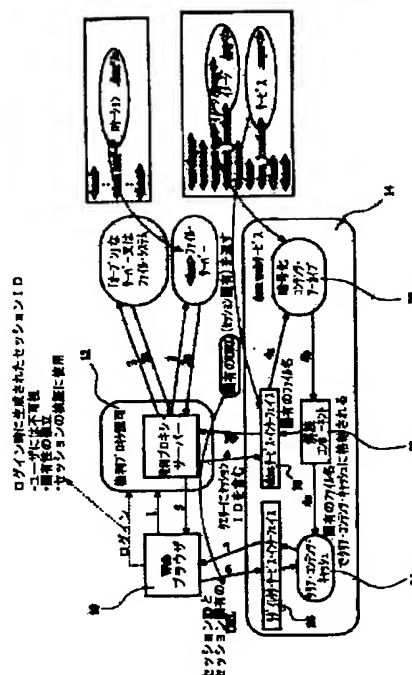
最終頁に続く

(54)【発明の名称】 プロキシ・サービス提供装置

(57)【要約】

【課題】 クライアント・プラットフォームと電子的なコンテンツを提供するリモート・コンテンツ・プロバイダの間のプロキシ・サービスを提供する装置を提供する。

【解決手段】 の装置は、コンテンツ・プロバイダの電子コンテンツに対するクライアント・プラットフォームの要求を受信して解釈する手段と、前記要求をコンテンツ・プロバイダに送信し、要求されたコンテンツに適した情報操作／ポリシー実施リモート・サーバーのロケーションを表す少なくとも1つのマーカを含むデータを受け取る手段と、前記1つ又は複数のマーカを解釈し、情報操作／ポリシー実施サービスの要件が満足された場合に前記コンテンツのクリア・コンテンツ・バージョンを前記クライアント・プラットフォームに送信するという要求を前記クライアント・プラットフォームに代わって送信する手段を備えている。



【特許請求の範囲】

【請求項1】 1つ又は複数のクライアント・プラットフォームと1つ又は複数のリモート・プラットフォームの間のプロキシ・サービスを提供する装置であって、

(a) リモート・プラットフォームの電子的なコンテンツ又は情報に対するクライアント・プラットフォームの要求を受信し解釈し、前記要求を前記リモート・プラットフォームに送信し、データを受け取る機能、または

(b) 前記リモート・プラットフォームに提供される典型的な情報又はコンテンツであるデータをクライアント・プラットフォームから受け取る機能のいずれか又は両方を行う手段を備え、

前記データは、要求又は提供された情報又はコンテンツに適した情報操作／ポリシー実施リモート・サービスのロケーションを表す少なくとも1つのマーカを含んでおり、

前記装置は、前記1つ又は複数のマーカを解釈し、情報操作／ポリシー実施サービスの要件が満足された場合に、

(a) 前記情報又はコンテンツのクリア・コンテンツ・バージョンを前記クライアント・プラットフォームに提供するという要求を前記クライアント・プラットフォームに代わって送信する機能、または

(b) 前記情報又はコンテンツのクリア・コンテンツ・バージョンを前記リモート・ロケーションに提供するという要求を適切な情報操作ポリシー実施サービスに送信する機能のいずれか又は両方を行う手段、

を備えるよう構成されたプロキシ・サービス提供装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、一般に電子権利管理に関し、特に情報技術ネットワーク環境専用の権利管理方式や他の情報操作ポリシーをサポートする柔軟なプラットフォームに関する。

【0002】

【従来の技術】 著作権は特定の種類の作品の原作者に与えられる知的所有権であり、原作者は著作権によってその作品の様々な利用法を管理できる。著作権は、文学、戯曲、音楽、美術の作品、出版物、録音物、映画（ビデオを含む）、放送（有線放送、衛星放送を含む）の原作を保護するためのものであり、著作権によって提供される権利は、保護の対象となる作品の複製、翻案、複製の配布、公演、放送などの様々な領域に及ぶ。また、多くの場合、著者には自分の作品であることを特定される権利と、自分の作品の毀損や変形に異議を唱える権利がある。さらに、録音物、映画、コンピュータ・プログラムの著作権所有者には貸与の権利が与えられるので、このような作品を公に貸し出すことによって実施するには著作権所有者から交付されたライセンスが必要になる。

【0003】 近年、録音物、文学作品、映画などのコン

テンツの電子的な保存がますます一般的になってきており、レコード店や書店などの小売店ではこのような電子コンテンツの商品流通が従来から行われている。情報技術ネットワークを介した電子コンテンツの商品流通には多くの利点があるが、このようなコンテンツの作者や流通業者に広く採用されているわけではない。その主な理由は、結果としてこのようなコンテンツをサード・パーティーが不法に複製、販売、配布しやすくなるのではないかという懸念である。このために、電子コンテンツの不当な複製を防止する技術的な防護策の開発に向けて多大な努力が払われてきた。

【0004】 デジタル・コンテンツは不法な複製が比較的容易であり、このことがコンテンツ・プロバイダにとっては好都合でもあり、不都合でもある。すなわち一方でコンテンツをできるだけ広く配布できるのは望ましいが（それによって価値が高まり、大きな利益の獲得も見込まれる）、依然として販売ごとに確実に支払いがあること、つまり著作権が侵害されないことを望んでいる。前述のような著作権侵害を防止するために、コンテンツ・プロバイダはデジタル保護方式（通常は暗号化技術に基づく）を採用する傾向がある。この方式は、a) 消費者には使いにくく配布の制限が難しい、b) 管理に費用がかかる、c) 同等のコンテンツをユーザーが操作しやすい無料の不法な方式によって無効化される恐れがある。

【0005】 既知の保護方式の1つはMicrosoft Digital Media Systemから提供されており、電子コンテンツがキーを伴って提供される。ユーザーは、正規のキー・サーバーから対応するキーを取得しないとコンテンツを再生できない。この方式の主な欠点は、ユーザーの再生装置との結び付きが強いことである。つまり、この方式で保護されたコンテンツを再生する場合は、専用の装置が必要になる。

【0006】 一般に、既知のデジタル権利管理及び保護方式には、作品の実質的な暗号化が含まれており、複製や複製されたコンテンツの再生が難しくなっている。現在使用されているデジタル権利管理（DRM: Digital rights management）技術は、ユーザーにはセキュア・コンテナとしても知られている。すなわち、この技術によって独自のファイル・フォーマットを定義し、その中で任意のメディア・ファイルをセキュアにカプセル化する。

【0007】 例えば、米国特許第6138119号に権利管理データ構造を定義、利用、操作するための技術が示されている。この明細書では、セキュアなデジタル・コンテナの概念を使用してデジタル・コンテンツの安全でセキュアな保存と転送を実現している。このようなコンテナは改ざんが難しいので、例えば、テキスト、グラフィック、実行可能ソフトウェア、オーディオやビデオなど、任意の形式のデジタル情報をパッケージ化するの

に利用できる。ただし、この方法ではセキュアなコンテンツを利用できる状況が限定される。

【0008】別のシステムでは、特定のメディア・フォーマット（Adobe（商標）PDFなど）に対して「プラグイン」セキュリティ機能を提供する。ソフトウェア・プラグイン・ビジネス・モデルは、ビデオやオーディオ（接続可能なcodec）、マルチメディア（プログラムを「拡張」する接続可能な実行プログラム）、クリエイティビティ・ツール（画像処理ツールを拡張するフィルタ）、Webブラウザなど、他の特定の市場で長年にわたってアプリケーションの拡張に使用されてきたが、現在ではAdobe Acrobat（商標）のみがセキュリティ機能を提供しており、サード・パーティーの開発者はAcrobat TMを使用して特定のフォーマットで機能するDRMを一律に開発できる。ただし、このシステムで使用する方法は、ターゲット・フォーマット（PDF）の機能によって制限される。つまり、この方法ではセキュリティを保証できるフォーマットが一種類に限定され、メディアの種類が限定される。

【0009】デジタル情報製品のプロバイダ、仲介業者、消費者は、情報製作者が知的所有権（IPR）を提示し、IPRポリシー（特に卸売業者、小売業者、ライブラリなどの仲介業者が情報を操作する規則を表すポリシー）を主張する一貫したプラットフォームのない「ポリシー実施の断片化」に悩まされている。このような情報をユーザー向けに表示し、ポリシーを解釈して実施するための一貫したプラットフォームは存在しない。ネットワーク・トランザクションの途中で公表できる私的なデータの送信と再利用に関わる消費者も、やはり一貫したプラットフォームを用意してその制御下で個人的な情報を操作するポリシーを実施しているわけではない。

【0010】一般に、情報バリュー・チェーンに関わるユーザーは、操作する情報の取扱いについて要求するポリシーと受け取った情報の取扱い又は処理についてのポリシーを提示してから情報を受け取ることを希望している。既知の技術では、この問題を一貫した体系的な方法で解決することはできない。

【0011】コンテンツのフィルタリングと適応のためにプロキシ・サービスを利用するという概念が知られている（「プロキシ」は、広義では単に「代理に付与された権限」を意味する）。例えば、望ましくないコンテンツの広告などを除去するための規則に基づくフィルタリングは、新たに発生した作業である。特に米国特許第5,996,011号では、ネットワークを介してコンピュータが受け取るデータから特定のデータをフィルタで除去することによって、受け取ったデータへのアクセスを制限するシステム及び方法について記述している。1つの実施態様では、インターネットに接続されたコンピュータが受け取るWorld Wide Webページ

から好ましくないテキスト・データ又は対象となるテキスト・データをフィルタリングするコンピュータベースの方法が示されている。米国特許第6,119,165号には、インターネット又はインターネット環境において、多くのクライアントをサポートするプロキシ・サーバーに機能を追加し、クライアントの特性に基づいて特定のクライアントにソフトウェア・モジュールを提供できるようにするシステムに関する記述がある。こうしてダウンロードされたモジュールは、プロキシ・サーバーとクライアントとの双方向通信リンクをセットアップしたクライアントによって実行される。双方向リンクによって、例えばクライアント・プラットフォームのウィンドウを使用したクライアント側でのステータス表示が可能になり、ウィルス・スキャン、コンテンツのフィルタリング、帯域幅利用など、プロキシ・サーバーの現在のステータスを表示できる。他のアプリケーションでは、ダウンロードされたモジュールによって組織の掲示板、ニュース・チャンネル、一般的なソフトウェア・パッチの提供元を構築できる。

【0012】米国特許第5,987,606号には、インターネット・コンピュータ・ネットワークからリモート・インターネット・サービス・プロバイダのサーバーによって取得され、ローカル・クライアント・コンピュータに転送されるインターネット・コンテンツをフィルタリングするシステムが示されている。このシステムでは、包含的なフィルタや排他的なフィルタなどの少なくとも1つのフィルタリング方式と、許可されるサイト又は除外されるサイトのリストなどの少なくとも1つのフィルタリング要素をローカル・クライアント・コンピュータで生成された個々のインターネット要求と照合する。この場合はISPサーバーにフィルタリング方式が実装されているが、一般にこの種のフィルタリング・サービスや適応サービスはクライアント側、サーバー、両者の中間点のいずれに適用してもよい。さらに、フィルタリングと適応はダウンストリーム・コンテンツ（クライアント・プラットフォームがサーバーから受け取るコンテンツ）に限定する必要はない。つまり、プライバシーや匿名を保証するためにユーザー入力に適応するプロキシ・サービスが存在する。

【0013】

【発明が解決しようとする課題】ただし、既知のプロキシ・サービスはいずれも情報操作ポリシーの適用（特に著作権の管理と行使のサービス）の実際的な介入ポイントを提供しない。前述のとおり、一般に著作権ポリシーを実施する既知のメカニズムでは、通常クライアント側で特別な「読み出し」ソフトウェアを使用し、コンテンツに関するエンドユーザーの楽しみを損なう結果になるか、サーバー側で非常に限定的なコンテンツに依存するポリシー実施機能を使用し、エンドユーザが鑑賞できるコンテンツを制限してしまうことになる。専用のクライ

アント・アプリケーションには、プラットフォーム互換性やアプリケーション互換性による制限からユーザーの不便まで、多くの欠点がある。既知のサーバーベースのシステムにも、管理上の粒状性の問題からコンテンツの柔軟性の問題まで、多くの弱点がある。

【0014】

【課題を解決するための手段】そこで、以上の問題を克服するための仕組みを考案した。こうして、本発明の第1の側面に従って、1つ又は複数のクライアント・プラットフォームと電子的なコンテンツ又は情報を提供する1つ又は複数のリモート・コンテンツ・プロバイダの間のプロキシ・サービスを提供する装置が提供される。

【0015】この装置は、コンテンツ・プロバイダの電子コンテンツに対するクライアント・プラットフォームの要求を受信して解釈する手段と、前記要求をコンテンツ・プロバイダに送信し、要求されたコンテンツに適した情報操作／ポリシー実施リモート・サーバーのロケーションを表す少なくとも1つのマーカを含むデータを受け取る手段と、前記1つ又は複数のマーカを解釈し、情報操作／ポリシー実施サービスの要件が満足された場合に前記コンテンツのクリア・コンテンツ・バージョンを前記クライアント・プラットフォームに送信するという要求を前記クライアント・プラットフォームに代わって送信する手段を備えている。

【0016】また、本発明の第1の側面に従って、1つ又は複数のクライアント・プラットフォームと電子コンテンツを提供する1つ又は複数のリモート・コンテンツ・サーバーの間のプロキシ・サービスを提供する方法も提供される。本方法には、コンテンツ・サーバーの電子コンテンツに対するクライアント・プラットフォームの要求を受信して解釈するステップと、前記要求をコンテンツ・サーバーに送信するステップと、要求されたコンテンツに適した情報操作／ポリシー実施リモート・サーバーのロケーションを表す少なくとも1つのマーカを含むデータを受け取るステップと、前記1つ又は複数のマーカを解釈するステップと、情報操作／ポリシー実施サービスの要件が満足された場合に前記コンテンツのクリア・コンテンツ・バージョンを前記クライアント・プラットフォームに送信するという要求を前記クライアント・プラットフォームに代わって送信するステップが含まれる。

【0017】本発明の第2の側面に従って、1つ又は複数のクライアント・プラットフォームと前記1つ又は複数のクライアント・プラットフォームから電子的なコンテンツ又は情報を受け取るように調整された1つ又は複数のリモート・プラットフォームの間のプロキシ・サービスを提供する装置が提供される。本装置は、リモート・プラットフォームに送信するデータが前記リモート・プラットフォームに提供される典型的な情報又はコンテンツであって提供される情報に適した情報操作／ポリ

ー実施リモート・サーバーのロケーションを表す少なくとも1つのマーカを含んでいる場合に、前記データをクライアント・プラットフォームから受け取る手段と、前記1つ又は複数のマーカを解釈する手段と、情報操作／ポリシー実施サービスの要件が満足された場合に前記情報のクリア・コンテンツ・バージョンを前記リモート・ロケーションに提供するという要求を適切な情報操作ポリシー実施サービスに送信する手段を備えている。

【0018】さらに、本発明の第2の側面に従って、1つ又は複数のクライアント・プラットフォームと前記1つ又は複数のクライアント・プラットフォームから電子的なコンテンツ又は情報を受け取るように調整された1つ又は複数のリモート・プラットフォームの間のプロキシ・サービスを提供する方法も提供される。本方法には、リモート・プラットフォームに送信するデータがリモート・プラットフォームに提供される典型的な情報又はコンテンツであって提供される情報に適した情報操作／ポリシー実施リモート・サーバーのロケーションを表す少なくとも1つのマーカを含む場合に、前記データをクライアント・プラットフォームから受け取るステップと、前記1つ又は複数のマーカを解釈するステップと、情報操作／ポリシー実施サービスの要件が満足された場合に前記情報のクリア・コンテンツ・バージョンを前記リモート・ロケーションに提供するという要求を適切な情報操作ポリシー実施サービスに送信するステップが含まれる。

【0019】このようにして、本発明はクライアント・プラットフォームと様々な権利管理ポリシーや情報操作ポリシーを伴う様々なコンテンツ・プロバイダとの中継点として利用できるプロキシ・サービスを提供し、それによってコンテンツ・プロバイダは自社の独自のポリシーを確実に実施できる。従って、本発明はクライアント・プラットフォームとクライアント・プラットフォームが機密性の高い情報や個人的な情報を送信する様々なリモート・ロケーションとの中継点として利用できるプロキシ・サービスを提供し、それによってクライアント・プラットフォームの機密性／匿名性に関する独自のポリシーを確実に維持できる。本発明に従った1つのプロキシ・サービスは2つの目的で利用できる。つまり、このようなサービスはクライアント・プラットフォームから受信するデータとクライアント・プラットフォームに送信するデータの両方を処理するように調整できる。

【0020】本プロキシ・サービスは、クライアント・プラットフォーム上にローカルに配置してもよい。ただし、「クライアント」が複数のプラットフォームを含む組織的なネットワークを備える場合は、本プロキシ・サービスをそのネットワーク内の中心に配置してもよい。あるいは、本プロキシ・サーバーをインターネットなどの情報技術ネットワークのリモート・ポイントに配置してもよい。

【0021】コンテンツ・サーバーは、本プロキシ・サービスからのコンテンツ要求に応答して1つ又は複数のマーカーを含むデータ・ストリームを返す。マーカーには、プロキシ・サービスがクライアント・プラットフォームにコンテンツの複製を送信する前に対話する必要がある他の1つ又は複数のサービスのロケーションの詳細情報（URLやDOIなど）が含まれる。このようなマーカーはデータ・ストリームに埋め込まれており、これを認識でき、解釈できるのはプロキシ・サービスの内部で提供される専用の手段に限定されるのが好ましい。

【0022】クライアント・プラットフォームがWebブラウザなどの場合は、情報操作／権利管理リモート・サーバーにコンテンツ要求を送信する際に（直接又は間接的に）、プロキシ・サービスは要求内にクライアント・プラットフォームに関連するデータ（セッションIDなど）を含むように調整されているのが好ましい。従って、情報操作／権利管理リモート・サーバーにクライアント・プラットフォームに関する情報が提供される。要求には、エンド・ユーザーに固有の詳細情報を含めることもできる（特に、エンド・ユーザーとクライアント・プラットフォームが別のエンティティであり、エンド・ユーザーとクライアント・プラットフォームが対話するための情報操作／権利管理サーバーに関連する特別な要件がない場合）。

【0023】情報操作／権利管理サーバーがプロキシ・サービスからコンテンツ要求を受信し、要求の合法性を検証すると、情報操作／権利管理サーバーはコンテンツのクリア・コンテンツ・バージョンを作成し、これをローカル又はリモートの特定のロケーションに保存し（できれば一時的に）、さらに前記ロケーションの詳細情報をプロキシ・サービスに返す。プロキシ・サービスは、コンテンツのクリア・コンテンツ・バージョンを保存するクライアント・プラットフォームのロケーションの詳細情報を送信するように調整できるのが好ましい。このことによって、情報操作／権利管理サーバーに関する特定の要件が満足された場合に、クライアント・プラットフォームは前記クリア・コンテンツの複製を取得できる。

【0024】情報操作／権利管理サーバーが採用するポリシーがコンテンツ・プロバイダと（当然のことながら）要求されたコンテンツの性質に依存するのは言うまでもない。情報操作／権利管理サービスがクライアント・プラットフォーム又はエンド・ユーザーに関連付けできることも明らかである。このことによって、クライアント・プラットフォームからリモート・ロケーションに送信される情報をプロキシ・サーバーによって操作し、適切な情報操作サービスを介して処理してから、前記リモート・ロケーションに送信できる。

【0025】

【発明の実施の形態】ここで、単に例として添付の図面

を参照しながら本発明の1つの実施態様について説明する。

【0026】図1を参照すると、Webブラウザ10（クライアント・コンピュータ・プラットフォーム（図示せず）からアクセス可能）、本発明に従ったプロキシ・サーバー12、デジタル権利管理（DRM）Webサービス14の間の典型的な接続（1つの例）が示されている。この接続は、通常はインターネットなどの情報技術ネットワークを介して行われる。矢印1、2、2a、3、3a、4、4a、4b、4c、4d、5、6、7は、以下に記述する典型的なプロセスでWebブラウザ10、プロキシ・サーバー12、DRM Webサービス14の間でやりとりする要求や応答の方向を示している。

【0027】最初のインスタンスでは、固有のセッションIDが生成された時点でWebブラウザ10がプロキシ・サーバー12にログインする。セッションIDはエンド・ユーザーには認識されず、後のプロセスでセッションの検証に使用される。

【0028】矢印1を参照すると、表示側クライアントすなわちWebブラウザ10はプロキシ・サーバー12にネットワーク・アドレス（例えばURLやDOI）を提示することでネットワーク・リソースの要求を行う。プロキシ・サーバー12は、ユーザーのワークステーションにローカルにも、企業や組織のネットワークに集中的にも、あるいはインターネットなどの情報技術ネットワークのリモート・ポイントにも配置できるのは言うまでもない。

【0029】プロキシ・サーバー12は、通常は、HTTPプロトコルを使用して、コンテンツ・サーバー16にリソースへの適切なネットワーク要求を送信する（矢印2）。コンテンツ・サーバー16は、通常はプロキシ・サーバー12とは別のロケーションに存在し、Webページなどのリソースを返す（矢印2a）。リソースは、一般にHTMLファイル又はより一般的なXMLファイルの形式をとる。リソース・ファイルには、他のリソースを呼び出すマークアップ・タグに類するものが埋め込まれており、プロキシ・サーバー12が提供する情報操作ポリシー又はデジタル権利管理に従った専用の処理のみによって取得できる。本発明のこの実施態様では、この種のマークアップ・タグは<DRM>オブジェクトとして記述される。プロキシ・サーバー12に送信される他の「オープン」なデータ・ストリーム内のこのような<DRM>オブジェクト・インスタンスは、プロキシ・サーバー12が埋め込みコンテンツ・オブジェクトのクリア（すなわち暗号化されていない）バージョンのロケーションを確認するために対話する必要がある他のWebリソースを参照する属性（URLやDOIなど）を備えている。

【0030】コンテンツ・サーバー16から受け取った

データ・ストリーム内に埋め込まれたマークアップ・タグにプロキシ・サーバー12が適応するのは言うまでもない。最初にプロキシ・サーバー12を通過することなくWebブラウザ10がコンテンツ・サーバー16から直接データ・ストリームを取得しようとしても、ブラウザが認識できるのはストリームの「オープン」な部分のみである。従って、マークアップ・タグを認識も解釈もできない（つまりWebブラウザ10はタグを無視する）。

【0031】プロキシ・サーバー12はコンテンツ・サーバー16からリソース・データ・ストリームを受け取ると、生成された一連の規則に従って受信したストリームを確認し、データ・ストリームに埋め込まれた1つ又は複数のマークアップ・タグを検出する。プロキシ・サーバー12は、例えばインターネット上のリモート・ポイントに配置された「drmファイル」のロケーションを示すプロパティをタグ本文から抽出するように調整されている。次に、プロキシ・サーバー12は指定された<DRM>ファイル（1つ以上）を要求し（矢印3）、受信する（矢印3a）。<DRM>ファイルでは、例えばXML構文を使用してもよい。プロキシ・サーバー12は、このファイルから実際のコンテンツ・オブジェクト（通常はセキュア・コンテナなどにパッケージ化されている）の“content_type”と“content_location”（例えばURL）を抽出する。

【0032】このサービスは、通常は“MIME”エンコード（image/jpegなど）を使用したcontent_typeを解釈し、このcontent_typeをプロキシ・サービスに登録した1つ又は複数のcontent_typeと比較する。content_typeがサービスに登録されたタイプの1つであれば、エンド・ユーザーに返す「クリア」なタグ構造が決定する。例えば、パッケージ化されたコンテンツがMIMEタイプ・イメージ/jpegの場合、変更されたタグ構造は“”のフォーマットでなければならない。つまり、エンド・ユーザーが（例えば登録ユーザーやライセンスを付与されたユーザーとして）リソースを使用できるようにする場合、プロキシ・サーバー12は次のように動作する。

【0033】ここで、プロキシ・サーバー12は、リモートDRM Webサービス14が指定されたリソースのセッションに固有の「クリアコンテンツ」バージョンを作成し、セッションに固有のURLを返すことを要求する（矢印4）。詳しく記述すると、drmサービス・インターフェイス18は<drm>ファイルの暗号化バージョンをdrm Webサービス14内の暗号化コンテンツ・アーカイブ20に配置する（矢印4a）。次に、コンテンツ・アーカイブ20は暗号化された<drm>ファイルを、やはりdrm Webサービス14内

に存在する解読コンポーネント22に送信する。解読コンポーネント22は、ファイルを解読してその「クリアコンテンツ」バージョンを作成する。このクリアコンテンツ・バージョンは、セッションに固有の（一時的な）固有のファイル名を使用して、やはりdrm Webサービス14内に存在するクリアコンテンツ・キャッシュ24に送信され（矢印4c）、キャッシングされる。また、固有のファイル名はdrmサービス・インターフェイス18に送信され、セキュアでないリソースのセッション固有のURLを生成してプロキシ・サーバー12に送信する（矢印4d）。

【0034】プロキシ・サーバー12は、（この場合は）MIME対応のフォーマットを使用して変更されたコンテンツ・ストリーム（例えばHTMLページ）を作成する。HTMLページは、drm Webサービス14が提供するセッション固有の一意のURLを特定するように再フォーマットされる。再フォーマットされたHTMLページは、ここでWebブラウザ10に返される（矢印5）。

【0035】次に、Webブラウザ10はdrm Webサービス14内のクリアコンテンツ・キャッシュ24にリダイレクタ・サービス・インターフェイス26を介して保存されるセキュアでないコンテンツを要求する（矢印6）。ブラウザの要求は、現在のブラウザ・セッションのみで有効なセッション固有のURLを含むクエリー・ストリングで構成される。リダイレクタ・サービス・インターフェイス26は、現在のブラウザ・セッションを確認してブラウザ10が送信するクエリー・ストリングに記述されるセッション固有のURLと比較する。セッションが一致し、クリア・コンテンツの一時記憶にタイムアウト規則があればその期限が切れていない場合に、リダイレクタ・サービス・インターフェイス26はWebブラウザ10にクリア・コンテンツを送信し、エンド・ユーザーはこれを利用できるようになる。

【0036】本発明は、プロキシベースの介入とコンテンツの適応という新しい概念に基づいており、情報操作ポリシーとデジタル権利管理ポリシーの解釈と実施を総括するプラットフォームを提供する。これは、特にポータルなどの場合に有効である。このような状況では、ユーザーが様々な表示環境を使用する関連の大規模なベースに対して、一貫した柔軟な方法でポリシーを適用する必要がある。換言すれば、本発明を使用すると、組織の異機種ネットワーク上にユーザー固有の情報操作ポリシー（著作権行使のポリシーなど）を一貫して適用できる。

【0037】本発明で採用する手法では、本質的にユーザー認証及び認可のプロセスとメカニズムをポリシー実施の実際の実装とは別に維持している。このことによって、組織又はコンテンツ・サービスは集中管理の企業データベースを利用して情報ポリシー（電子ジャーナルに

関する組織のサイト・ライセンスなど、特に組織内の様々なロールに様々なポリシーが適用される場合)を管理できる。

【0038】明細書の以上の部分では、本発明についてその特定の典型的な実施態様に関連して記述してきた。ただし、前述の請求項に示す本発明の精神と範囲を逸脱しない限り、その様々な変形や変更が可能なのは、当業者には明らかである。従って、本明細書と図面は制限を意味するものではなく例示を意図するものと見なす必要がある。

【0039】この発明は、例として次の実施形態を含む。

【0040】(1) 1つ又は複数のクライアント・プラットフォーム(10)と1つ又は複数のリモート・プラットフォーム(16)の間のプロキシ・サービス(12)を提供する装置であって、(a) リモート・プラットフォーム(16)の電子的なコンテンツ又は情報に対するクライアント・プラットフォーム(10)の要求を受信して解釈し、前記要求を前記リモート・プラットフォーム(16)に送信してデータを受け取る機能、または(b) 前記リモート・プラットフォーム(16)に提供される典型的な情報又はコンテンツであるデータをクライアント・プラットフォーム(10)から受け取る機能のいずれか又は両方を行う手段を備えており、前記データは要求又は提供された情報又はコンテンツに適した情報操作／ポリシー実施リモート・サービス(14)のロケーションを表す少なくとも1つのマーカーを含んでおり、前記装置は、前記1つ又は複数のマーカーを解釈し、情報操作／ポリシー実施サービスの要件が満足された場合に、(a) 前記情報又はコンテンツのクリア・コンテンツ・バージョンを前記クライアント・プラットフォームに提供するという要求を前記クライアント・プラットフォームに代わって送信する機能と、(b) 前記情報又はコンテンツのクリア・コンテンツ・バージョンを前記リモート・ロケーションに提供するという要求を適切な情報操作ポリシー実施サービスに送信する機能のいずれか又は両方を行う手段、を備える前記装置。

【0041】(2) プロキシ・サービス(14)による情報又はコンテンツの要求に回答して1つ又は複数のマーカーを含むデータ・ストリームを返し、マーカーにはプロキシ・サービス(12)がクライアント・プラットフォーム(10)にコンテンツの複製を送信する前に対話する必要がある他の1つ又は複数のサービスのロケーションの詳細情報が含まれる(1)に記載の装置。

【0042】(3) データ・ストリームにマーカーが埋め込まれており、プロキシ・サービス(12)の内部で提供される専用の手段のみによってマーカーを認識でき、解釈できる(2)に記載の装置。

【0043】(4) クライアント・プラットフォームが

Webブラウザ(10)などの場合、情報操作／権利管理リモート・サービス(14)に情報又はコンテンツ要求を送信する際に、プロキシ・サービス(12)が要求内にセッションIDなどのクライアント・プラットフォーム(10)に関連するデータを含むように調整される(1)から(4)のいずれかに記載の装置。

【0044】(5) 情報操作／権利管理サービス(14)がプロキシ・サービス(12)からコンテンツ要求を受信して要求の合法性を検証すると、コンテンツのクリア・コンテンツ・バージョンを作成し、ローカル又はリモートの特定のロケーション(24)に保存し、さらに前記ロケーションの詳細情報をプロキシ・サービス(12)に返す(1)から(4)のいずれかに記載の装置。

【0045】(6) 前記コンテンツのクリア・コンテンツ・バージョンが一時的に記憶される(5)に記載の装置。

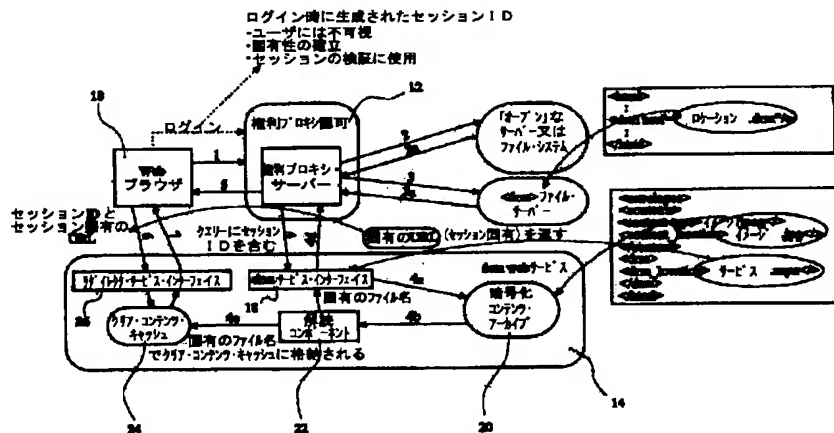
【0046】(7) プロキシ・サービス(12)がコンテンツのクリア・コンテンツ・バージョンを保存するクライアント・プラットフォーム(10)のロケーションの詳細情報を送信するように調整され、その結果、情報操作／権利管理サービス(14)に関する特定の要件が満足された場合にクライアント・プラットフォーム(10)が前記クリア・コンテンツの複製を取得できる(5)に記載の装置。

【0047】(8) 1つ又は複数のクライアント・プラットフォーム(10)と1つ又は複数のリモート・プラットフォーム(16)の間のプロキシ・サービス(12)を提供する方法であって、(a) リモート・プラットフォーム(16)の電子的な情報又はコンテンツに対するクライアント・プラットフォーム(10)の要求を受信して解釈し、前記要求を前記リモート・プラットフォーム(16)に送信してデータを受け取るステップと、(b) 前記リモート・プラットフォーム(16)に提供される典型的な情報又はコンテンツであるデータをクライアント・プラットフォーム(10)から受け取るステップのいずれか又は両方を含み、前記データに要求又は提供された情報又はコンテンツに適した情報操作／ポリシー実施リモート・サービス(14)のロケーションを表す少なくとも1つのマーカーが含まれており、さらに前記1つ又は複数のマーカーを解釈するステップと、情報操作／ポリシー実施のサービス(12)の要件が満足された場合に、(a) 前記情報又はコンテンツのクリア・コンテンツ・バージョンを前記クライアント・プラットフォーム(10)に提供するという要求を前記クライアント・プラットフォーム(10)に代わって送信するステップと、(b) 前記情報又はコンテンツのクリア・コンテンツ・バージョンを前記リモート・プラットフォーム(16)に提供するという要求を適切な情報操作ポリシー実施サービス(12)に送信するステッ

【符号の説明】

- 10 クライアント・プラットフォーム
12 プロキシ・サービス
14 情報操作／権利管理リモート・サービス
16 リモート・プラットフォーム

【图 1】



フロントページの続き

Fターム(参考) 5B017 AA07 BA06 CA16
5B085 AA08 AE02 AE23 BA07 BC02
BE04 BG04 BG07